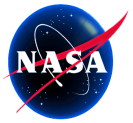


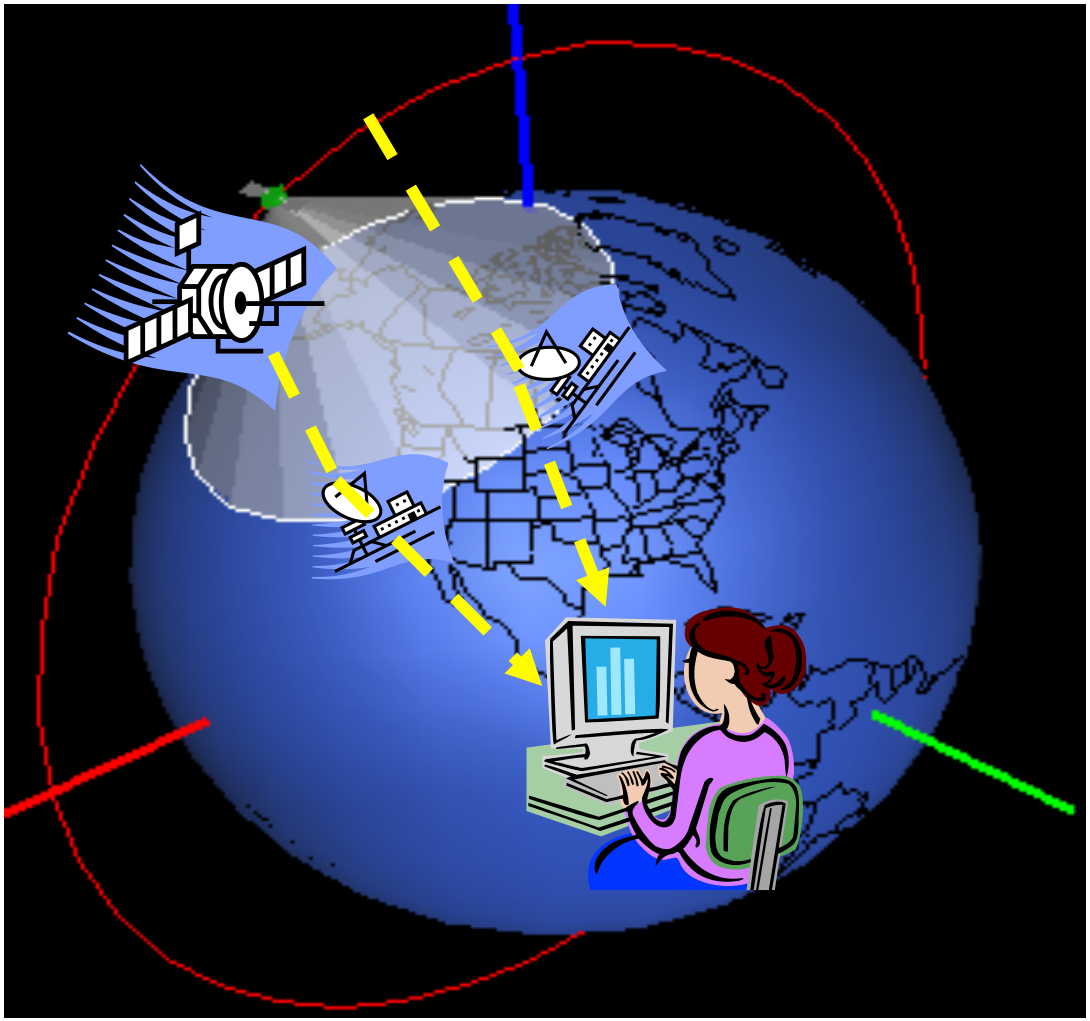
# Security Issues in Space Networks

Mohammad Atiquzzaman
School of Computer Science
University of Oklahoma

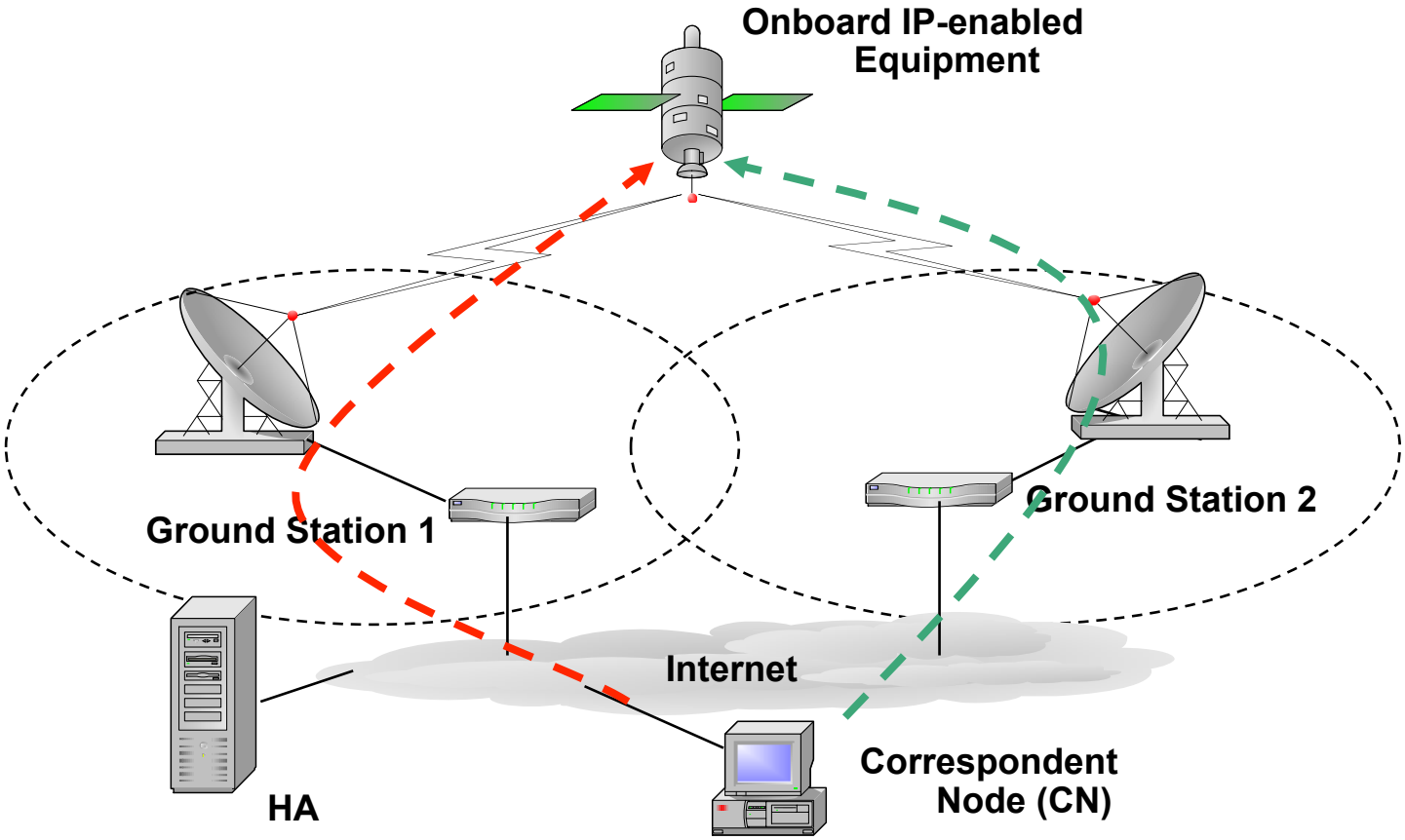
NASA Earth Science Technology Forum
June 21, 2011

# Motivation for mobility protocols

- Onboard Satellite equipments need to communicate with control centers
- Ground stations provide different IP prefix to Satellite
- Need to maintain continuous connectivity with remote computer



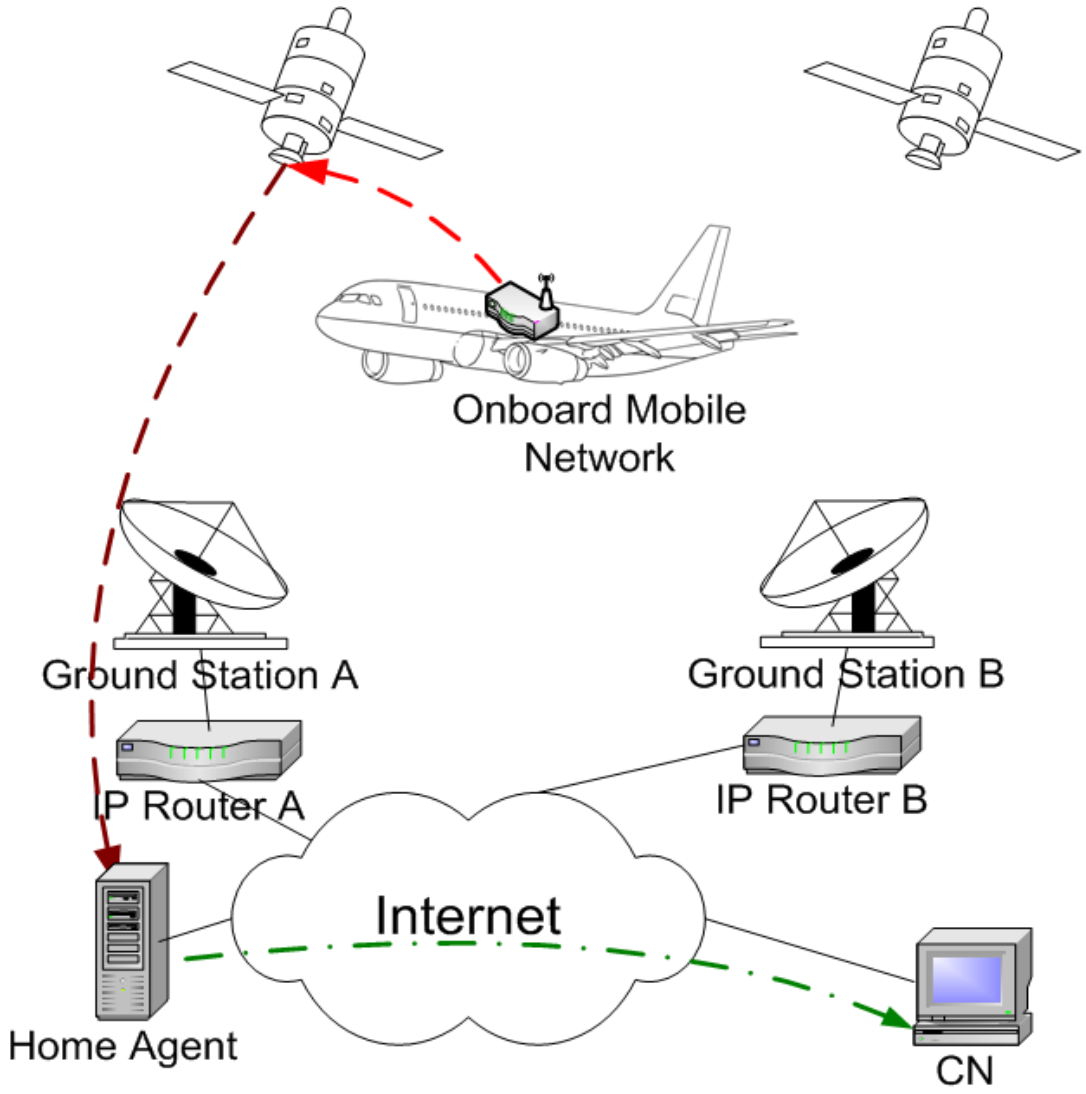
# Satellite as Mobile Host / Network




- Satellite with one or more onboard IP-enabled equipments acts as mobile host / network.
- Ground stations works as Access Points.

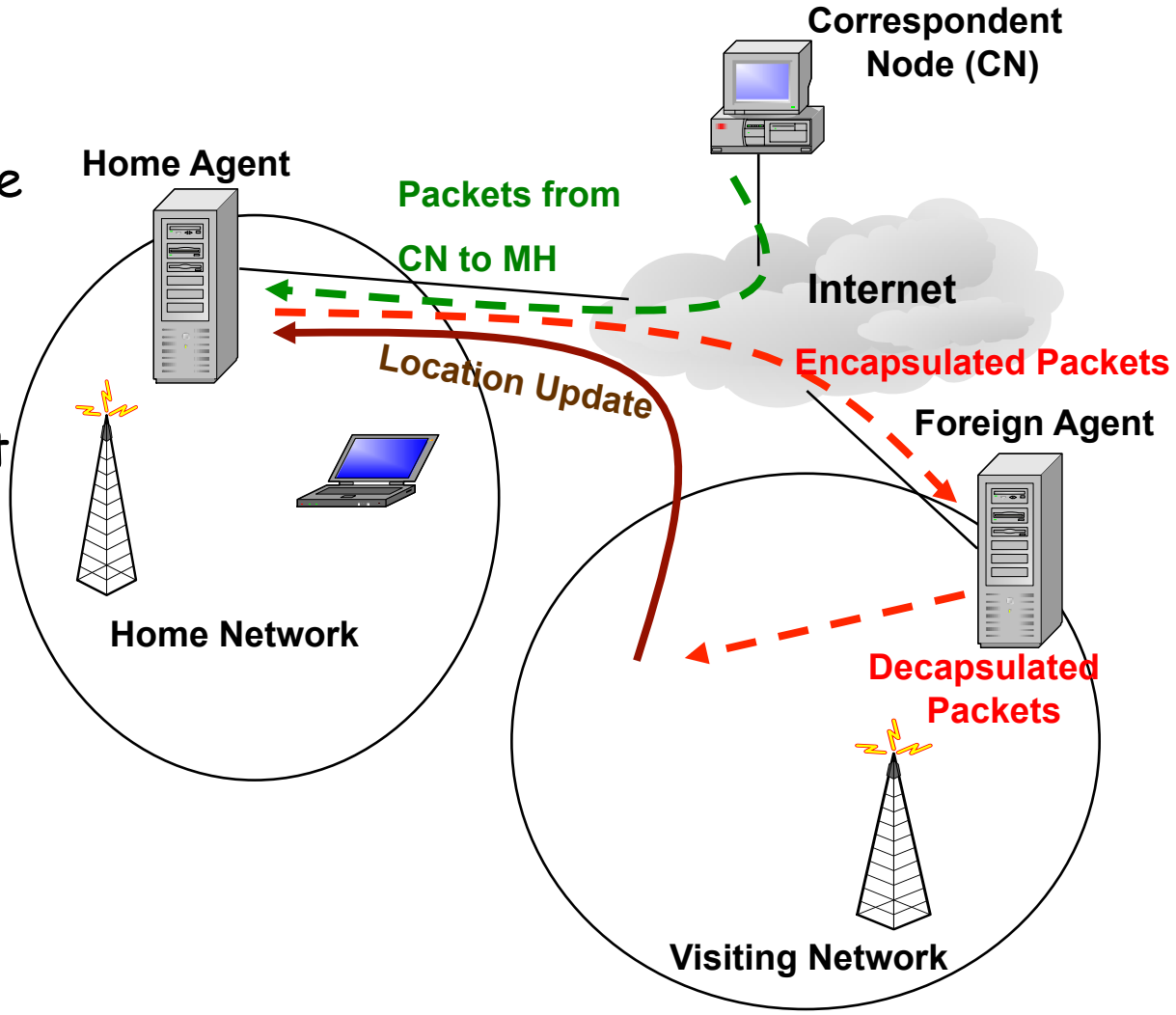
# Satellite as router

- Satellites can act as routers in the Internet.
- Can provide IP-connectivity to Mobile hosts / network in other spacecrafts or in remote location on earth.



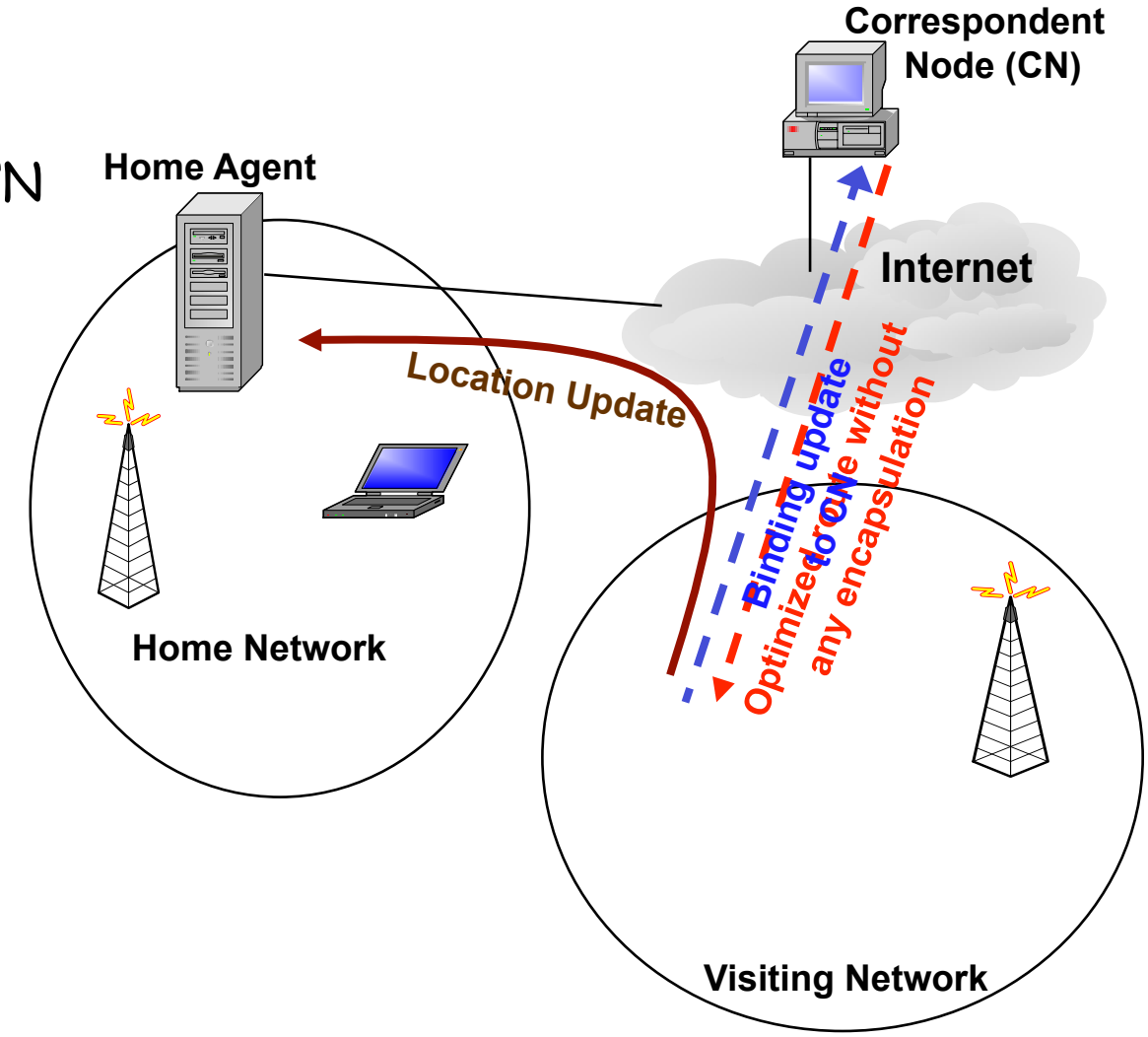
# IETF Solution to IP Mobility: Mobile IP

- Employs mechanism similar to postal service mail forwarding
- no route optimization
- All traffic passed through the home agent



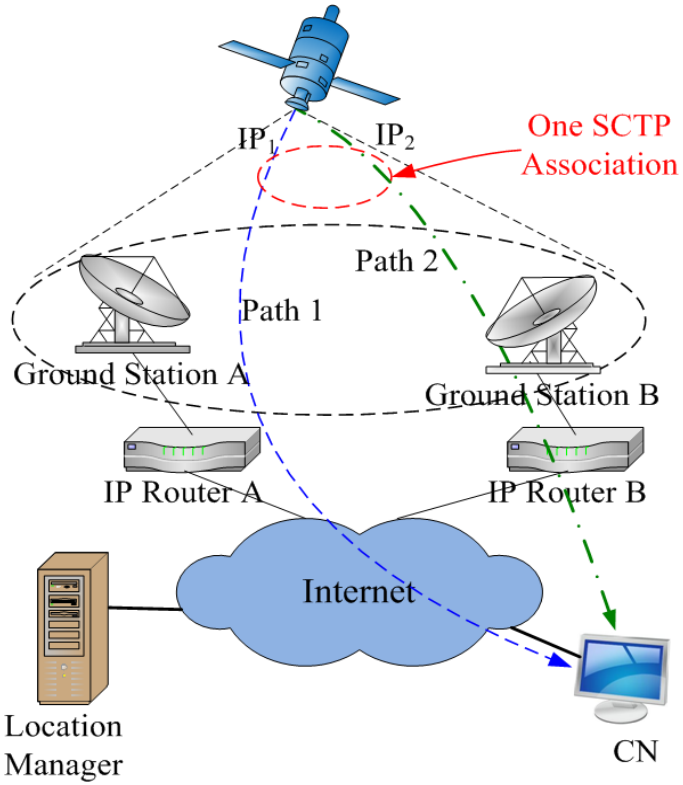
# Route optimization

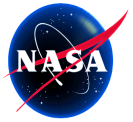
- After moving to new location, MH informs CN about its location though binding update
- Improved performance



# SIGMA

- An IP-diversity based approach developed in our lab
- Can be used in both terrestrial and space networks
- Uses Stream Control Transport Protocol (SCTP)

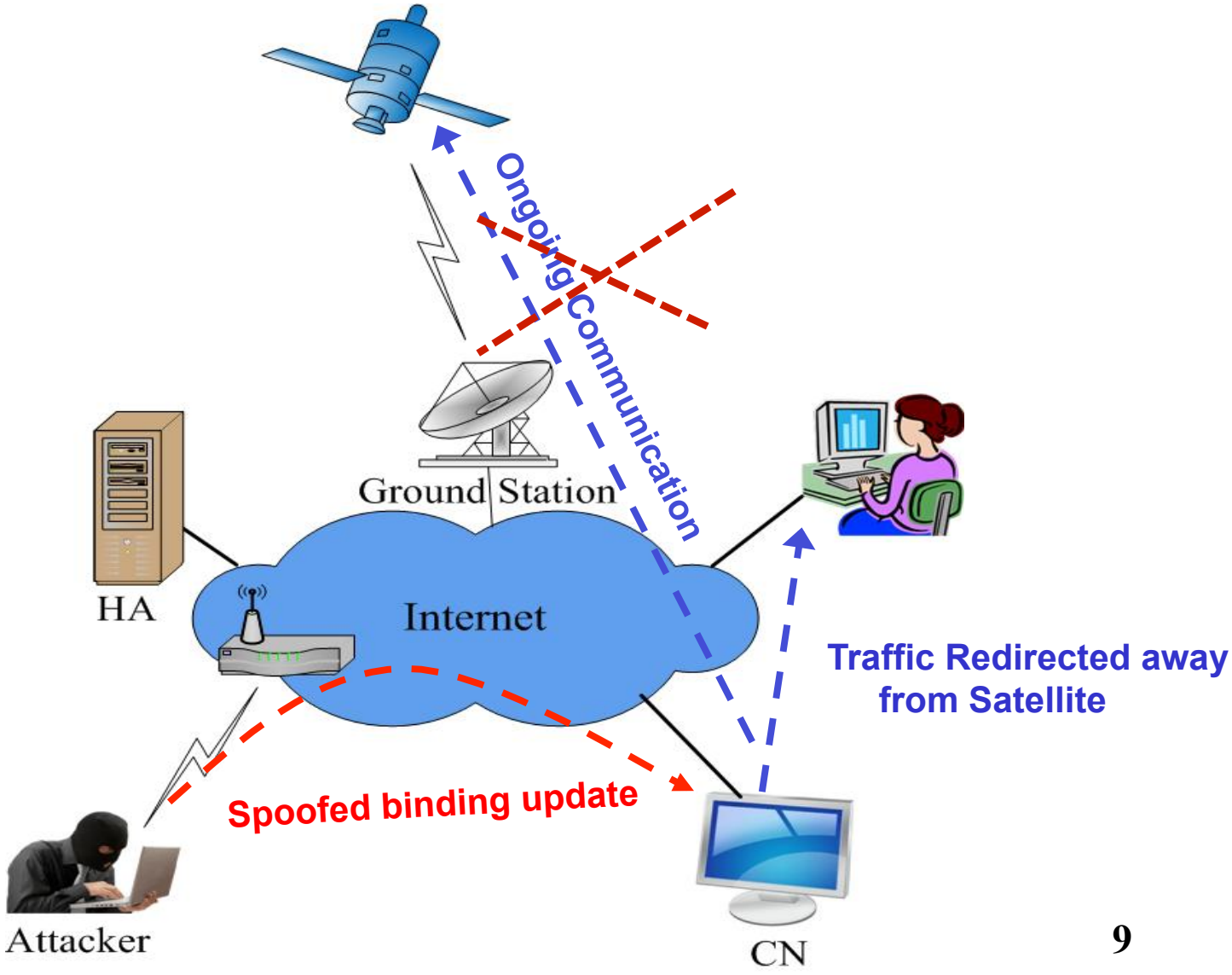




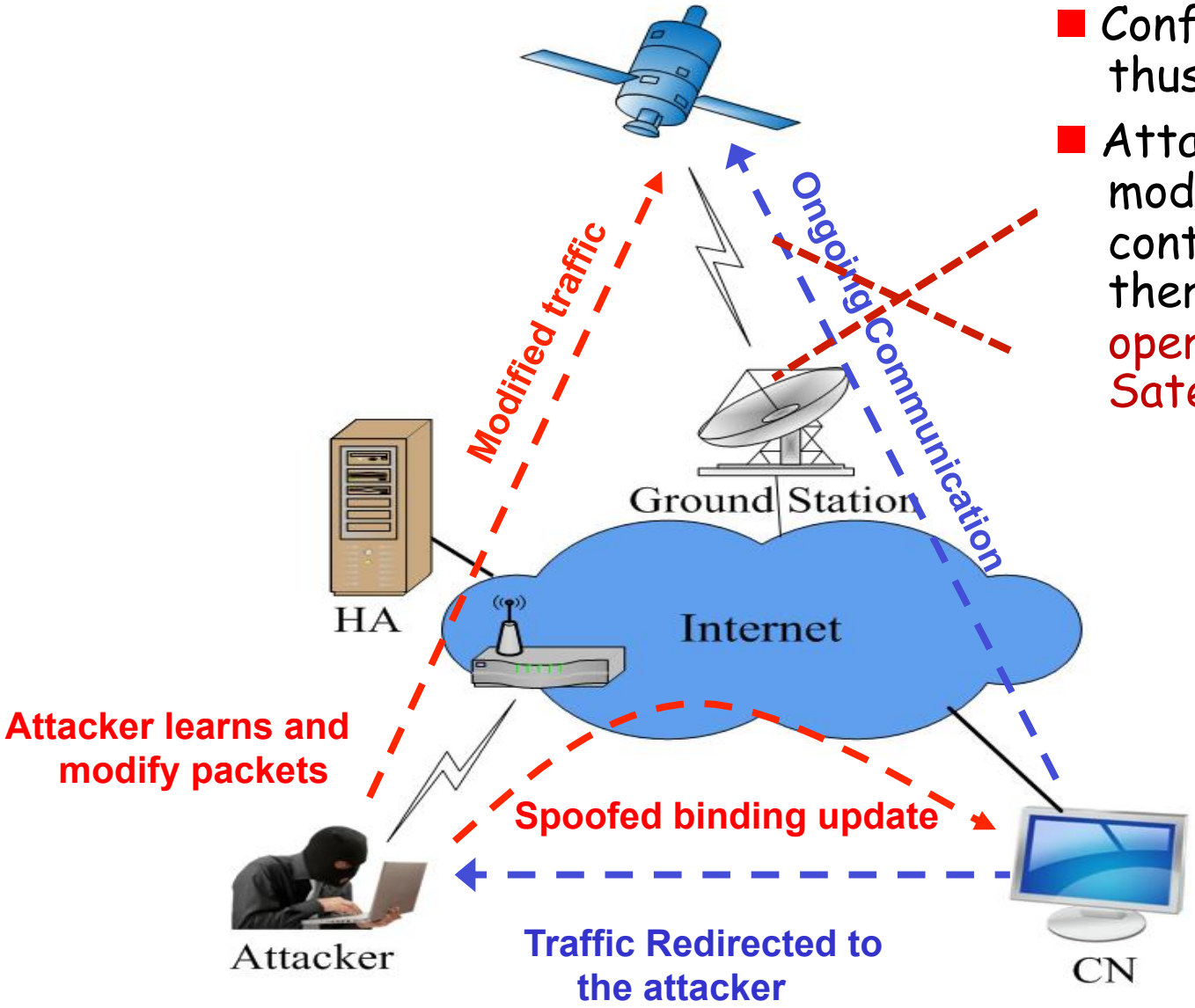
# Major Security Threats

- Seamless mobility and use of optimized route may introduce several security threats:
  - Traffic redirection attack
  - Man-in-the-middle attack
  - Bombing attack
  - Reflection attack
  - HA poisoning
  - Resource exhaustion

# Traffic Redirection Attack

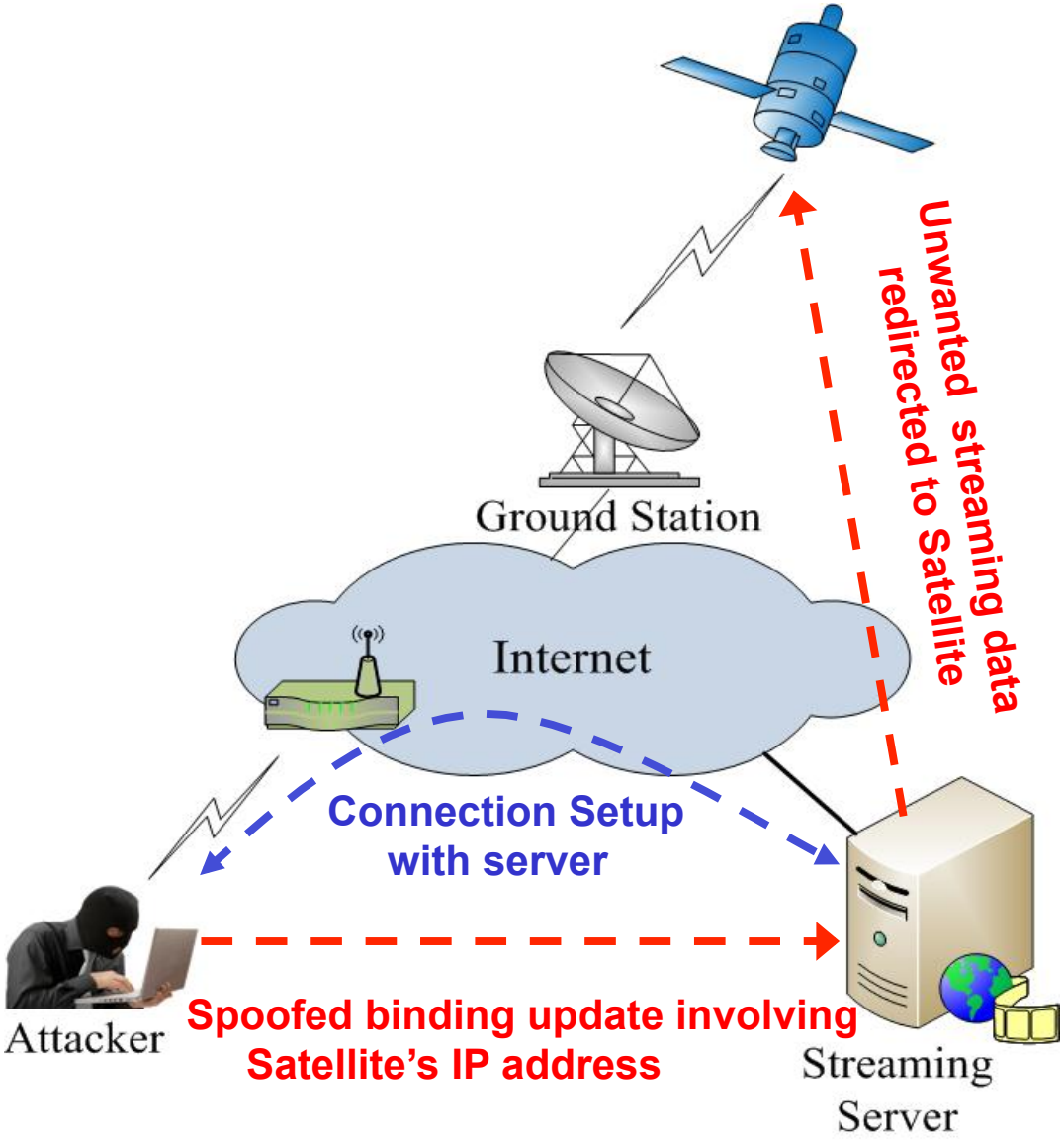


# Man-in-the-middle Attack



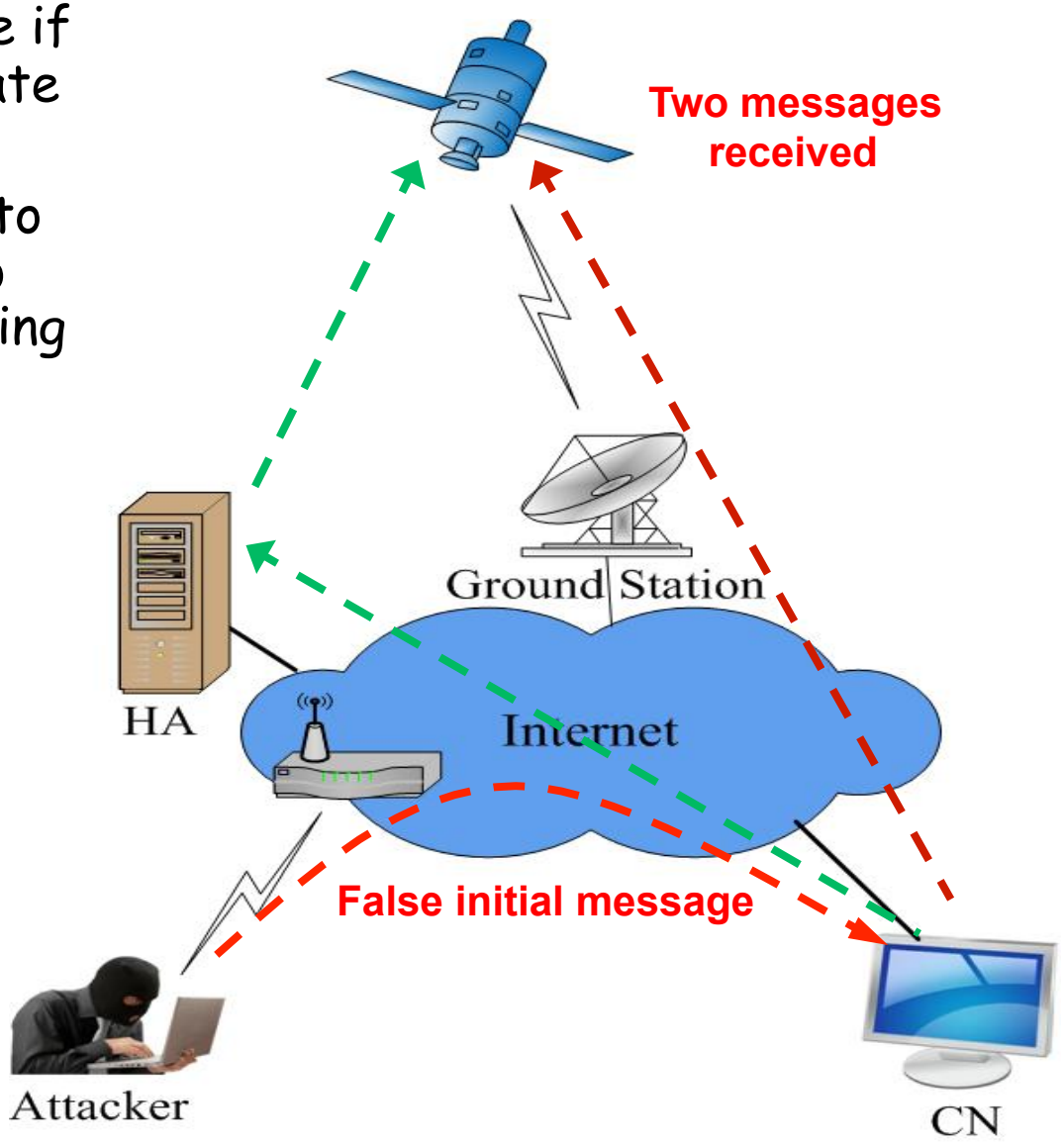

- Confidential data may thus be compromised.
- Attacker may send modified command and control message, thereby altering the operation sequence of Satellites.

# Bombing Attack

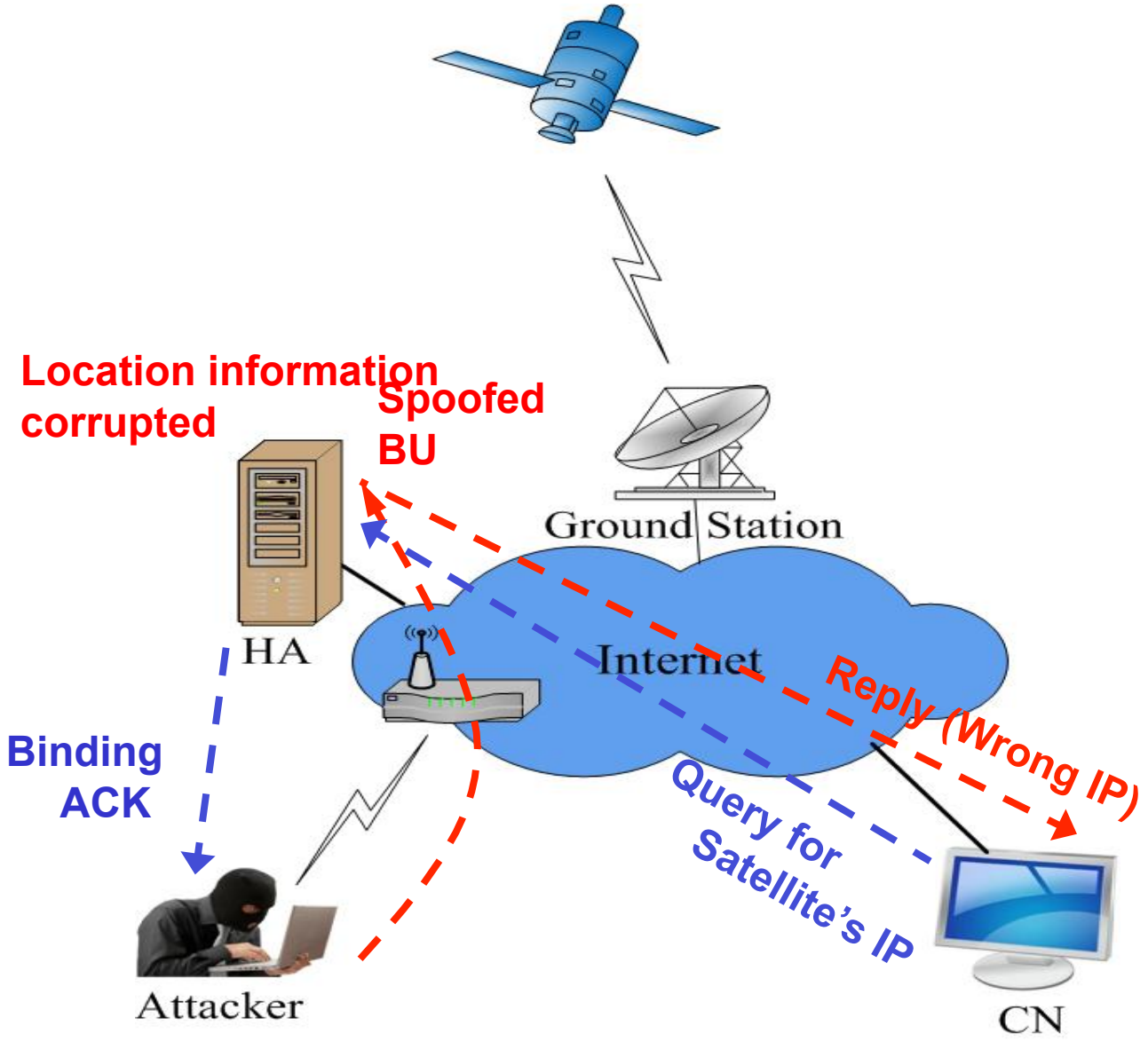


# Reflection Attack

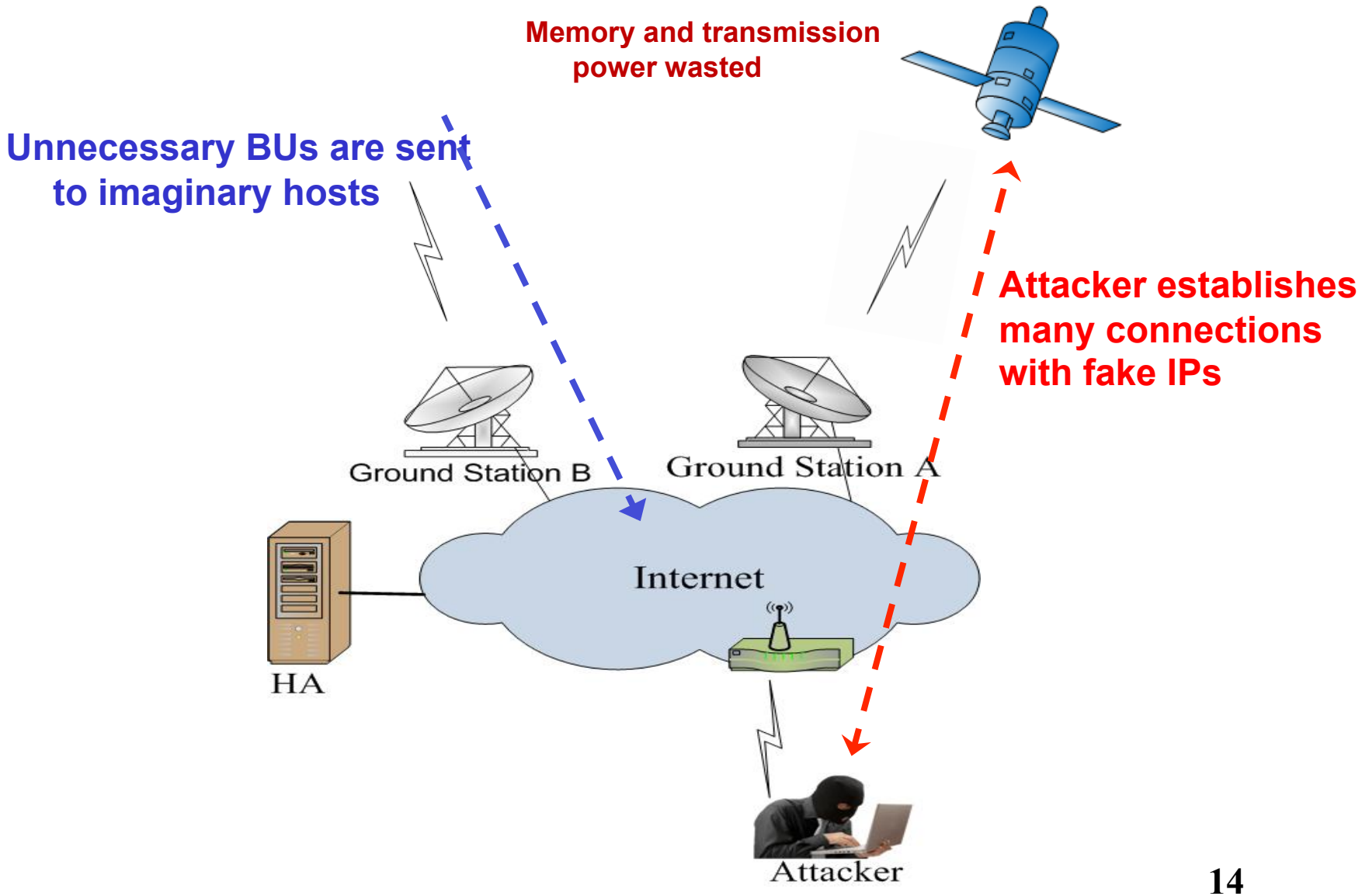
- This attack is possible if CN is allowed to initiate route optimization.
- Thus CN are induced to send two messages to the victim node, wasting its bandwidth.

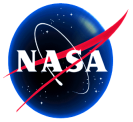


# Home Agent poisoning



# Resource Exhaustion



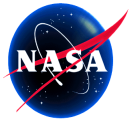


# Unnecessary Cryptographic Operations

- Attacker may trick MH to unnecessary complex cryptographic operations, thereby using up the resources and leading to denial-of-service attacks.

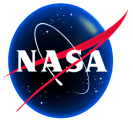
- These kinds of attack are very harmful for spacecrafts since they have limited processing power.

- The satellites may not be able to do legitimate operations and communication may be disrupted.



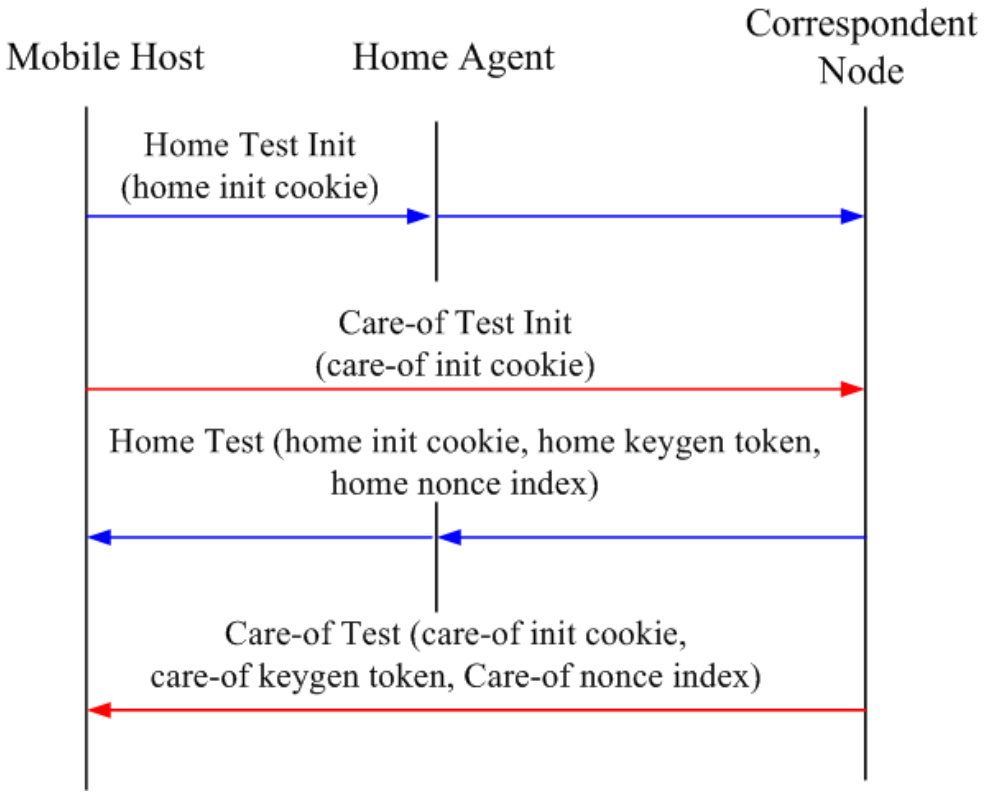
# Defense Mechanisms

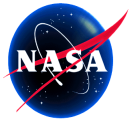
- Existing defense mechanisms:
  - Return Routability protocol
  - IPSec
    - Authentication Header (AH) protocol
    - Encapsulating Security Payload (ESP) protocol
  - Internet Key Exchange (IKE)-based schemes
  - Use of Cryptographically Generated Address
  - Stateless approach
  - Certificate based approach



# Return Routability Protocol

- Major threat: unauthenticated and forged binding updates.
- Return routability is proposed for Mobile IPv6.
- A node sending a binding update must prove its right to redirect the traffic.
- RR messages are exchanged among MH, CN and HA before binding updates are sent.

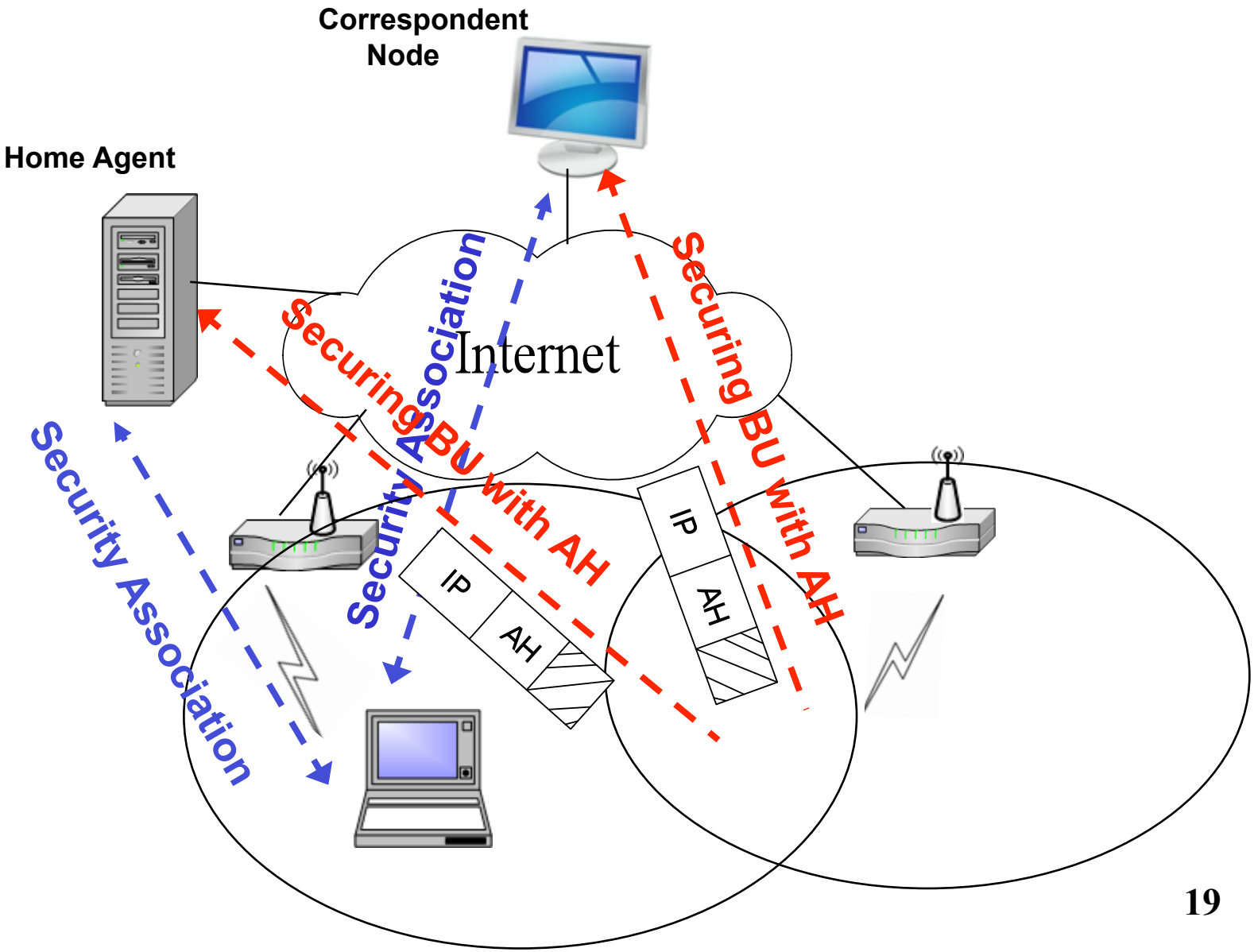


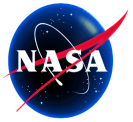


# Authentication Header (AH)

- AH guarantees connectionless integrity and data origin authentication of IP packets.
- First, security association are used to decide on security algorithms and parameters to be used for an outgoing packet / incoming packets.
- Next, BU is secured by AH which follows IP header.
- Use of such AH ensures that any attacker cannot fool the CN or the HA with spoofed BU.
- As a result, the traffic redirection attacks can be avoided.

# Use of Authentication Header (AH)

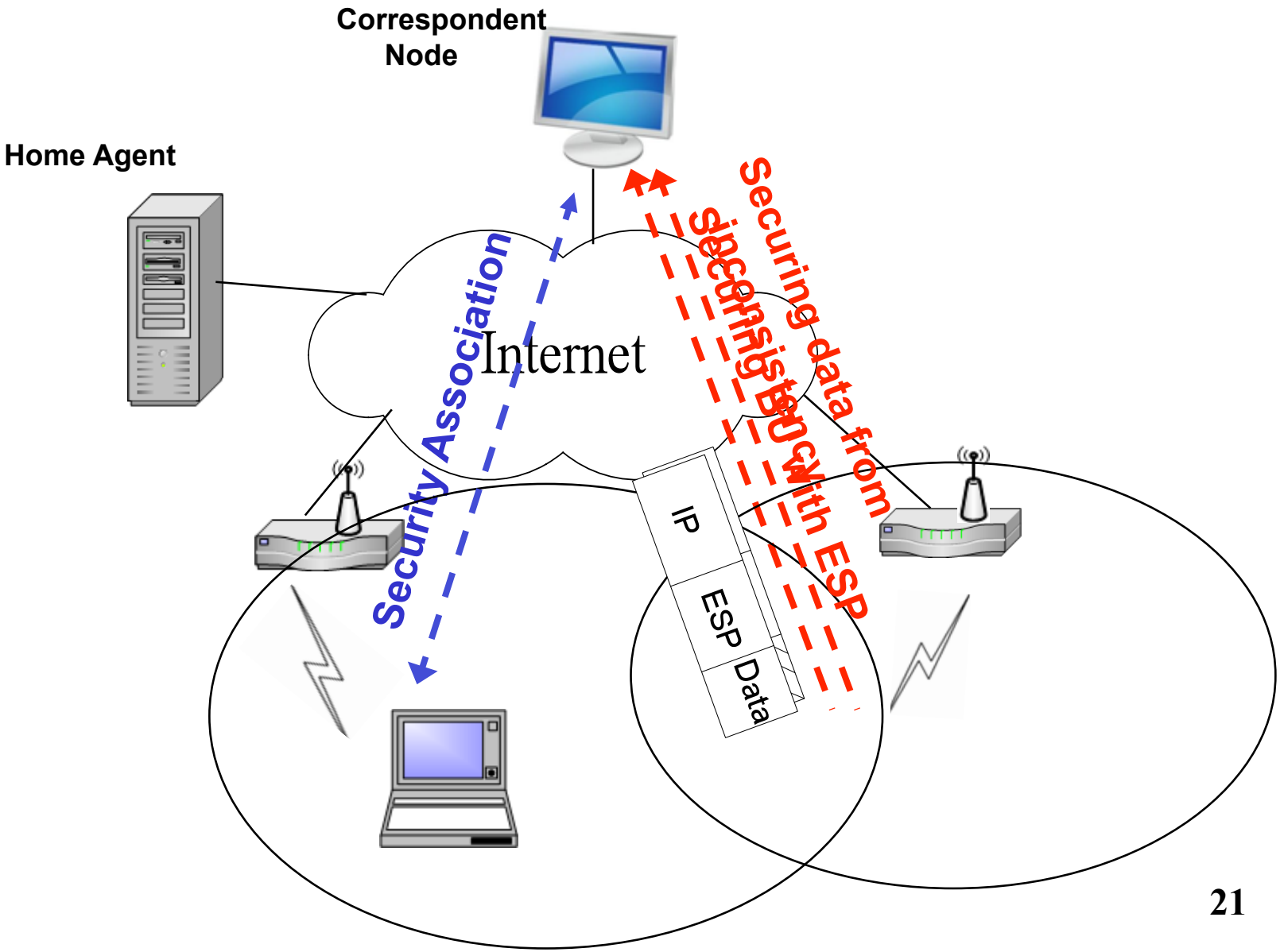


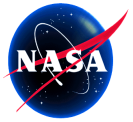


# Encapsulating Security Payload (ESP)

- AH protocol cannot ensure data integrity.
- However, ESP protocol can ensure data confidentiality as well as integrity in addition to authentication.
- ESP ensures privacy of data by encrypting the data.
- An encryption algorithm combines the data in the datagram with a key to transform it into an encrypted form.

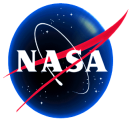
# Use of ESP


Correspondent Node
Home Agent
Internet
Security Association
Securing data from
IP
ESP
Data



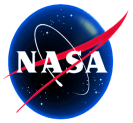
# IKE-based schemed

- Commonly used for mutual authentication and establishing and maintaining security associations for IPSec protocol suite.
- Ensures confidentiality, data integrity, access control, and data source authentication.
- IPSec maintains state information at the two ends of the data communication.
- IKE helps to dynamically exchange the secret key that is used as the input to the cryptographic algorithms.



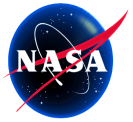
## Other possible approaches

- Use of Cryptographically Generated Address: To avoid redirection attack.
- Certificate based approach: authentication purpose.
- Stateless nodes: To avoid resource exhaustion.



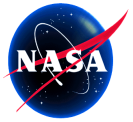
# Comparison

| Security Threats | Protection Mechanisms | Advantage | Limitations |
|---|---|---|---|
| Attack on BU (MH-HA) | IPSec ESP | Protects against certain types of traffic analysis and provides privacy | Does not protect against misbehaving MH that may use spoofed CoA in BU to launch DoS attacks |
| Attack on BU (MH-CN) | Return routability | Makes sure that the MH sending the BU has the right to use the CoA | Vulnerabilities possible if the attacker is on the path between HA and CN |
| Traffic redirection | AH protocol, CGA, frequently changing addresses | The BUs are authenticated using this IPSec protocol | Privacy and confidentiality are not ensured by AH protocol |
| Man-in-the-middle | PKI and secret key based approach | Difficult to break | Cryptographic operations needed to shared key |
| HA poisoning | AH or ESP | strong authentication | Computationally expensive |
| Spoofing BU | CGA | Works with a CA or any PKI | Higher processing cost and can suffer from resource exhaustion attacks |
| Resource exhaustion | Keeping MH or CN stateless | Can avoid DoS attacks | May introduce delay for valid requests |



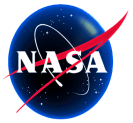
# Conclusion

- Discussed the IP-security issues in space networks.
- Explained possible security vulnerabilities that may lead to wastage of all-important bandwidth and processing power of the expensive IP-enabled devices onboard the Satellite / aircrafts.
- Analyzed the existing and possible defense mechanisms that can prevent or mitigate these security vulnerabilities along with their pros and cons.



# Acknowledgements


- The research reported in this paper is supported by National Aeronautics and Space Administration (NASA).




# Thank You